Application case serial number 09/312,150

Attached are the search results (from commercial databases) for your case.

Color tags mark patents/articles which appear to be most relevant to the case.

[redacted]

Pls call if you have any ?s or suggestions for additional terminology,
or a different approach to searching the case.

Prepared for: Examiner Arvind Moorthy

By : Carol Wong, EIC2100, 305-9729

Pk2
4B14

Date : 5/20/03

```
File 347:JAPIO Oct 1976-2003/Jan(Updated 030506)
         (c) 2003 JPO & JAPIO
File 350:Derwent WPIX 1963-2003/UD,UM &UP=200331
         (c) 2003  Thomson Derwent
? ds

Set     Items   Description
S1     217678   KEY OR CIPHER??? ? OR CYPHER??? ? OR ALGORITHM??? ?
S2       2894   (SESSION? ? OR SUBSESSION? OR DATA OR CATEGORY OR ONE()TIM-
             E)(1W)S1
S3       3691   (PUBLIC OR TWO)(1W)S1 OR TWO()KEY? ? OR KEY()PAIR? ?
S4         53   ASYMMETRIC(1W)S1
S5       1849   (MASTER OR GROUP OR COMMON)(1W)S1
S6       2601   S2(5N)(DATA OR INFORMATION OR PACKET? ? OR MESSAGE? ? OR F-
             ILE OR FILES OR CONTENT)
S7         24   S2 AND S3:S4 AND S5
S8         44   S2(3N)(COPY??? ? OR COPIE? ? OR DUPLICAT? OR REPLICAT? OR -
             REPRODUC????? ? OR FACSIMILE? OR MIRROR? ? OR CLONE? ? OR CLO-
             NING? OR VERSION? ?)
S9          3   S8 AND S5
S10        26   S7 OR S9
S11        26   IDPAT (sorted in duplicate/non-duplicate order)
S12        25   IDPAT (primary/non-duplicate records only)
? t12/9/all

 12/9/1     (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2003  Thomson Derwent. All rts. reserv.

014277465    **Image available**
WPI Acc No: 2002-098167/200213
Related WPI Acc No: 2002-303727
XRPX Acc No: N02-072518
  Secure computer communication method in Internet, involves establishing
  common   session   key  between server and client based on decrypted
  cipher-text
Patent Assignee: INGRIAN SYSTEMS INC (INGR-N); BERI S (BERI-I); BONEH D
  (BONE-I); SHACHAM H (SHAC-I)
Inventor: BERI S; BONEH D; SHACHAM H
Number of Countries: 096  Number of Patents: 003
Patent Family:
Patent No     Kind   Date     Applicat No    Kind   Date     Week
WO 200197443   A2  20011220  WO 2001US18878  A   20010612  200213  B
AU 200169794   A   20011224  AU 200169794    A   20010612  200227
US 20020087884  A1  20020704  US 2000211023   A   20000612  200258
                             US 2000211031   A   20000612
                             US 2001877655   A   20010608

Priority Applications (No Type Date): US 2001877655 A 20010608; US
  2000211023 P 20000612; US 2000211031 P 20000612
Patent Details:
Patent No  Kind Lan Pg   Main IPC     Filing Notes
WO 200197443  A2 E  46 H04L-009/30
   Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA
   CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN
   IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ
   PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
   Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR
   IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW
AU 200169794  A        H04L-009/30   Based on patent WO 200197443
US 20020087884 A1       G06F-012/14   Provisional application US 2000211023
```

Abstract (Basic): WO 200197443 A2

NOVELTY - A Rivest-Shamir-Adleman (RSA) **public key** is transmitted from a server after receiving the request from the client. A random string (R) is encrypted using the **public key** to output a cipher-text C' to a server. The server decrypts the text using the RSA private key based on which a **common session key** is established between the server and client.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Initial handshake establishing method;

(b) Rivest-Shamir-Adleman **public** /private **key** generation method;

(c) Secure network communication system;

(d) Rivest-Shamir-Adleman decryption method;

(e) Recorded medium for storing Rivest-Shamir-Adleman decryption program;

(f) Electromagnetic medium

USE - For providing secure computer communication between server and client in Internet, for E-commerce and financial web sites.

ADVANTAGE - The security protection service in network is enhanced and improved by the initial SSL handshake in the server. The efficiency of decrypting the cipher-text message is increased at low processing cost, thus the bandwidth and the overall efficiency of the network is increased.

DESCRIPTION OF DRAWING(S) - The figure shows the flowchart explaining the secure computer communication method.

pp; 46 DwgNo 1/6

Title Terms: SECURE; COMPUTER; COMMUNICATE; METHOD; ESTABLISH; COMMON; SESSION; KEY; SERVE; CLIENT; BASED; CIPHER; TEXT

Derwent Class: T01; W01

International Patent Class (Main): G06F-012/14; H04L-009/30

International Patent Class (Additional): G06F-011/30; H04L-009/00; H04L-009/32

File Segment: EPI

Manual Codes (EPI/S-X): T01-D01A; T01-N01D; T01-S01C; T01-S03; W01-A05A

**12/9/2 (Item 2 from file: 350)**

DIALOG(R)File 350:Derwent WPIX



013988904 **Image available**

WPI Acc No: 2001-473118/200151

**Method for materializing key agreement protocol with key confirmation possible to confirm communizing of diffie-helman type key**

Patent Assignee: UNIV INFORMATION & COMMUNICATIONS (UYIN-N)

Inventor: KIM G J; SONG B Y

Number of Countries: 001 Number of Patents: 001

Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week | |
|---|---|---|---|---|---|---|---|
| KR 2001008103 | A | 20010205 | KR 200066178 | A | 20001108 | 200151 | B |

Priority Applications (No Type Date): KR 200066178 A 20001108

Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| KR 2001008103 | A | | 1 | H04L-009/30 | |

Abstract (Basic): KR 2001008103 A

NOVELTY - A method for materializing a key agreement protocol with key confirmation possible to confirm communizing of a Diffie-Helman type key is provided to supply the security by uniting a temporary personal key and a long-term personal key or by uniting only the temporary personal keys.

DETAILED DESCRIPTION - A method for materializing a key agreement protocol with key confirmation possible to confirm communizing of a Diffie-Helman type key includes a few steps. In the first step(210) substance A generates a pair of temporary keys. In the second step(212) substance A sends the temporary **public key** and a certificate of the **public key** to the substance B. In the third step(214) substance B certifies the temporary **public key** of substance A. In the fourth step(216) substance B generates a pair of temporary keys. In the fifth step(218) substance B generates k', a **common key** and k, a **session key** . In the sixth step(220) substance B calculates the message certifying code. In the seventh step(222) substance B sends the temporary **public key** , the certificate of the **public key** and the message certifying code to substance A. In the eighth step(224) substance A certifies the temporary **public key** of substance B. In the ninth step(226) substance A generates k', a **common key** In the tenth step(228) substance A calculates the message certifying code. In the eleventh step(230) substance A certifies the temporary **public key** of substance B. In the twelfth step(232) substance A calculates the temporary **public key** of substance B. In the thirteenth step(234) substance A calculates k, a **session** key . In the fourteenth step(236) substance A sends the message certifying code to substance B. In the fifteenth step(238) substance B calculates mA', a message certifying code. In the sixteenth step(240) substance B certifies the message certifying code of substance A.

pp; 1 DwgNo 1/10

Title Terms: METHOD; KEY; AGREE; PROTOCOL; KEY; CONFIRM; POSSIBILITY; CONFIRM; TYPE; KEY

Derwent Class: W01

International Patent Class (Main): H04L-009/30

File Segment: EPI

Manual Codes (EPI/S-X): W01-A05A

**12/9/3 (Item 3 from file: 350)**

DIALOG(R)File 350:Derwent WPIX



013439802 **Image available**

WPI Acc No: 2000-611745/200058

XRPX Acc No: N00-452992

**Content material encryption for cryptographic system, involves creating session key based on which content material is encrypted and communicated to destination devices, with partial keys corresponding to device**

Patent Assignee: KONINK PHILIPS ELECTRONICS NV (PHIG )

Inventor: EPSTEIN M A; PASIEKA M; ROSNER M

Number of Countries: 022 Number of Patents: 005

Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week | |
|---|---|---|---|---|---|---|---|
| WO 200059154 | A1 | 20001005 | WO 2000EP1895 | A | 20000306 | 200058 | B |
| EP 1080558 | A1 | 20010307 | EP 2000909313 | A | 20000306 | 200114 | |
| | | | WO 2000EP1895 | A | 20000306 | | |
| CN 1304604 | A | 20010718 | CN 2000800901 | A | 20000306 | 200163 | |
| KR 2001043748 | A | 20010525 | KR 2000713105 | A | 20001122 | 200168 | |
| JP 2002540721 | W | 20021126 | JP 2000608543 | A | 20000306 | 200307 | |

Priority Applications (No Type Date): US 99434156 A 19991104; US 99126168 P 19990325
Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| WO 200059154 | A1 | E | 22 | H04L-009/08 | |
| Designated States (National): CN JP KR | | | | | |
| Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE | | | | | |
| EP 1080558 | A1 | E | | H04L-009/08 | Based on patent WO 200059154 |
| Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE | | | | | |
| CN 1304604 | A | | | H04L-009/08 | |
| KR 2001043748 | A | | | H04L-009/08 | |
| JP 2002540721 | W | | 22 | H04L-009/08 | Based on patent WO 200059154 |

Abstract (Basic): WO 200059154 A1

NOVELTY - A **session key** (221) is created based on combination of each of public keys (251a,261a,271a,281a) corresponding to destination devices (250,260,270,280). Partial keys (225-228) corresponding to the destination devices, are created. The content material (201) is encrypted based on **session key** , and the encrypted content material is communicated to the destination device with its corresponding partial key.

DETAILED DESCRIPTION - Partial key is configured to provide decryption key corresponding to the **session key** , when combined with the private keys (251b,261b,271b,281b) of the corresponding destination device and the public group keys (212a). The partial key of a destination device includes product of public keys of other destination devices. INDEPENDENT CLAIMS are also included for the following:

(a) source device;

(b) method to decrypt encrypted content material;

(c) destination device

USE - For use in cryptographic systems to encrypt and decrypt content materials.

ADVANTAGE - Multiple device key exchange facilitates common encryption of content material for selective decryption by one or more of the device. Thus computation requirements are minimized at a destination node for a multiple device key exchange. By supplying partial key and **group key** that is combined with a private key of each destination device to form decryption key, the same encryption of content material is distributed to multiple destination devices. Each destination device receives appropriate partial key corresponding to its particular private key.

DESCRIPTION OF DRAWING(S) - The figure shows the key exchange between source and multiple destination devices.

Content material (201)

**Public group key** (212a)

**Session key** (221)

Partial keys (225-228)

Destination devices (250,260,270,280)

Public keys (251a,261a,271a,281a)

Private keys (251b,261b,271b,281b)

pp; 22 DwgNo 3/5

Title Terms: CONTENT; MATERIAL; ENCRYPTION; CRYPTOGRAPHIC; SYSTEM; SESSION; KEY; BASED; CONTENT; MATERIAL; ENCRYPTION; COMMUNICATE; DESTINATION; DEVICE; KEY; CORRESPOND; DEVICE
Derwent Class: W01
International Patent Class (Main): H04L-009/08
International Patent Class (Additional): G06F-012/14

File Segment: EPI
Manual Codes (EPI/S-X): W01-A05A

**12/9/4 (Item 4 from file: 350)**
DIALOG(R)File 350:Derwent WPIX


013058500 **Image available**
WPI Acc No: 2000-230368/200020
Related WPI Acc No: 1991-364231; 2000-230366; 2000-230367
XRPX Acc No: N00-173575
**Encryption** data key **designation device in encryption communication system, encrypts or decodes communication sentence by common encryption process using** master public key
Patent Assignee: HITACHI LTD (HITA )
Number of Countries: 001 Number of Patents: 001
Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week |
|---|---|---|---|---|---|---|
| JP 2000049769 | A | 20000218 | JP 9038221 | A | 1990022 | 200020 B |
| | | | JP 99228238 | A | 19900221 | |

Priority Applications (No Type Date): JP 9038221 A 19900221; JP 99228238 A 19900221
Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| JP 2000049769 | A | | 20 | H04L-009/08 | Div ex application JP 9038221 |

Abstract (Basic): JP 2000049769 A
NOVELTY - A **data key** is decoded using key designation information and user secret key information. By using a **public key** encryption process, first key information is generated from decoded **data key** . A communication sentence is encrypted or decoded by a common encryption process using **master public key** .
USE - In encryption communication system for data communication between data terminal and host computer.
ADVANTAGE - Illegal decipherment of encrypted communication sentence is prevented. DESCRIPTION OF DRAWING(S) - The figure shows the system assembly of encryption communication system.
Dwg.1/10
Title Terms: ENCRYPTION; DATA; KEY; DESIGNATED; DEVICE; ENCRYPTION; COMMUNICATE; SYSTEM; DECODE; COMMUNICATE; SENTENCE; COMMON; ENCRYPTION; PROCESS; MASTER; PUBLIC; KEY
Derwent Class: W01
International Patent Class (Main): H04L-009/08
File Segment: EPI
Manual Codes (EPI/S-X): W01-A05A

**12/9/5 (Item 5 from file: 350)**
DIALOG(R)File 350:Derwent WPIX


012891318 **Image available**
WPI Acc No: 2000-063153/200006
Related WPI Acc No: 2000-063151; 2000-063154
XRPX Acc No: N00-049446
**Establishing secure facsimile communication method for data transmission**
Patent Assignee: CERTICOM CORP (CERT-N)
Inventor: LINDSAY S K; VADEKAR A

Number of Countries: 001  Number of Patents: 001
Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week | |
|---|---|---|---|---|---|---|---|
| CA 2260483 | A1 | 19990727 | CA 2260483 | A | 19990127 | 200006 | B |

Priority Applications (No Type Date): GB 981702 A 19980127
Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| CA 2260483 | A1 | E | 20 | H04N-001/44 | |

Abstract (Basic): CA 2260483 A1

NOVELTY - The method consists transmitting set of attributes includes **public key** and signature algorithm between correspondents and attributes, followed by exchanging (34) of **public key** certificates between correspondents. A **common session key** is established between correspondent, key, identification and **public key** information of the correspondent. Finally, encrypting a massage using **common key** for transmission.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM includes a secure facsimile.

USE - Secure facsimile data transmission.

ADVANTAGE - The user can decide which fax transmissions are sent or received in a secure mode and allows secure transmission of data. Allows ease of maintenance by keeping database of each module configuration.

DESCRIPTION OF DRAWING(S) - The drawing shows a state machine representation of a session establishment protocol.

Exchange (34)

pp; 20 DwgNo 3/4

Title Terms: ESTABLISH; SECURE; FACSIMILE; COMMUNICATE; METHOD; DATA; TRANSMISSION
Derwent Class: W01; W02
International Patent Class (Main): H04N-001/44
International Patent Class (Additional): H04L-009/30
File Segment: EPI
Manual Codes (EPI/S-X): W01-A05A; W02-J03C6

**12/9/6  (Item 6 from file: 350)**
DIALOG(R)File 350:Derwent WPIX


012842680  **Image available**
WPI Acc No: 2000-014512/200002
XRPX Acc No: N00-011320

**Computer-based exchange method of cryptographic key - involves forming session key by using first hash function, whereby input size of hash function comprises at least one term formed through exponential function of public network key with first random number**

Patent Assignee: SIEMENS AG (SIEI )
Inventor: HORN G; KESSLER V; MUELLER K
Number of Countries: 020  Number of Patents: 005
Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week | |
|---|---|---|---|---|---|---|---|
| DE 19822795 | A1 | 19991125 | DE 1022795 | A | 19980520 | 200002 | B |
| WO 9960747 | A2 | 19991125 | WO 99DE1365 | A | 19990506 | 200003 | |
| DE 19822795 | C2 | 20000406 | DE 1022795 | A | 19980520 | 200021 | |
| EP 1080557 | A2 | 20010307 | EP 99932641 | A | 19990506 | 200114 | |
| | | | WO 99DE1365 | A | 19990506 | | |
| JP 2002516521 | W | 20020604 | WO 99DE1365 | A | 19990506 | 200239 | |

JP 2000550242 A 19990506

Priority Applications (No Type Date): DE 1022795 A 19980520
Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| DE 19822795 | A1 | | 23 | H04L-009/00 | |
| WO 9960747 | A2 | G | | H04L-009/00 | |
| Designated States (National): JP US | | | | | |
| Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE | | | | | |
| DE 19822795 | C2 | | | H04L-009/00 | |
| EP 1080557 | A2 | G | | H04L-009/00 | Based on patent WO 9960747 |
| Designated States (Regional): DE FR GB | | | | | |
| JP 2002516521 | W | | 76 | H04L-009/08 | Based on patent WO 9960747 |

Abstract (Basic): DE 19822795 A

The method involves forming a first value (gt) from a first random number (t) by using a producing element (g) of a finite group of elements, and a first message (M1), comprising at least the first value, is send by the first computer unit to a second computer unit (N). A **session key** (K) is formed in the second computer unit by using a first hash function (hl), whereby a first input quantity of the first hash function comprises at least one first term which is formed through an exponential function of the first value with a secret network key (s).

The session being (IF) is also formed in a first computer unit (U), whereby a second input quantity of the first hash function comprises at least one second term which is formed through an exponential function of a **public** network **key** (gns) with the first random number. A fourth input size is formed in the first computer unit by using a second hash function (h2) or the first hash function, whereby a third input size for the first hash function or the second hash function comprises one or further sizes for producing the fourth input size, from which the **session key** can be uniquely derived. A first signature function (SigU) is used in the first computer unit to form a signature term from, at least the fourth input size. A third message (M3) is send from the first computer unit to the second computer unit, which comprises at least the signature term of the first computer unit, whereby the signature term is verified in the second computer unit.

USE - In security module, especially for mobile communications system, PC communication, etc.

ADVANTAGE - Does not require **common** secret **key** .

Dwg.1/3

Title Terms: COMPUTER; BASED; EXCHANGE; METHOD; CRYPTOGRAPHIC; KEY; FORMING ; SESSION; KEY; FIRST; HASH; FUNCTION; INPUT; SIZE; HASH; FUNCTION; COMPRISE; ONE; TERM; FORMING; THROUGH; EXPONENTIAL; FUNCTION; PUBLIC; NETWORK; KEY; FIRST; RANDOM; NUMBER
Derwent Class: P85; T01; U21; W01; W02
International Patent Class (Main): H04L-009/00; H04L-009/08
International Patent Class (Additional): G06F-012/14; G06F-015/163; G09C-001/00; H03M-007/00; H04K-001/00
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): T01-D01; T01-H01C2; T01-H07C; U21-A05A; W01-A05; W01-A05A; W01-A07G; W01-B05A; W02-C03C; W02-L05

**12/9/7 (Item 7 from file: 350)**
DIALOG(R)File 350:Derwent WPIX


012056730 **Image available**

WPI Acc No: 1998-473641/199841
XRPX Acc No: N98-369942
**Key management method used in encryption communication system - involves obtaining** session **key at receiving side user apparatus by performing decoding of receiving addition** data **using** session **encryption** key
Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE )
Number of Countries: 001 Number of Patents: 001
Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week | |
|---|---|---|---|---|---|---|---|
| JP 10200520 | A | 19980731 | JP 973644 | A | 19970113 | 199841 | B |

Priority Applications (No Type Date): JP 973644 A 19970113
Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| JP 10200520 | A | | 10 | H04L-009/08 | |

Abstract (Basic): JP 10200520 A

The method involves setting-up a system **public** presentation **key** and a system secret key by a key management system (3,4) or key generation system, during system construction. The user public presentation information and user confidential information are generated, during system subscription of a user, by a user apparatus. The system **public** -presentation **key** and user public presentation information are exhibited, after generating the **master key** specifying a communication person.

The registration management of system secret key and user confidential information or **master key** are performed to one or several key management system. When performing encryption communication, a calling side user apparatus generates the **session** encryption **key** using the data containing the **master key** specifying communication person, and the data indicating time components such as time information. The addition data are generated by performing encryption of data containing the **session key** . Then, the addition data are transmitted to a receiving side user apparatus. The receiving side user apparatus generates the **session** encryption **key** , by performing decoding of the received addition data using **session** encryption **key** .

ADVANTAGE - Eliminates infringing on user's privacy by **duplicating session key** .

Dwg.1/6
Title Terms: KEY; MANAGEMENT; METHOD; ENCRYPTION; COMMUNICATE; SYSTEM; OBTAIN; SESSION; KEY; RECEIVE; SIDE; USER; APPARATUS; PERFORMANCE; DECODE ; RECEIVE; ADD; DATA; SESSION; ENCRYPTION; KEY
Derwent Class: W01
International Patent Class (Main): H04L-009/08
File Segment: EPI
Manual Codes (EPI/S-X): W01-A05A

**12/9/8 (Item 8 from file: 350)**
DIALOG(R)File 350:Derwent WPIX


010937154 **Image available**
WPI Acc No: 1996-434104/199643
XRPX Acc No: N96-365714
**Key encryption method for telecommunications method enabling wire-tapping warrants - defining** session **key for public and secret keys of monitored and monitoring parties respectively and which is valid for set time interval**

Patent Assignee: TELCORDIA TECHNOLOGIES INC (TELC-N); BELL COMMUNICATIONS RES INC (BELL-N)
Inventor: LENSTRA A K; WINKLER P M; YACOBI Y
Number of Countries: 019 Number of Patents: 005
Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week | |
|---|---|---|---|---|---|---|---|
| WO 9628913 | A1 | 19960919 | WO 96US2477 | A | 19960223 | 199643 | B |
| US 5633928 | A | 19970527 | US 95402176 | A | 19950310 | 199727 | |
| EP 872064 | A1 | 19981021 | EP 96911216 | A | 19960223 | 199846 | |
| | | | WO 96US2477 | A | 19960223 | | |
| JP 11502035 | W | 19990216 | JP 96527619 | A | 19960223 | 199917 | |
| | | | WO 96US2477 | A | 19960223 | | |
| CA 2215050 | C | 20001226 | CA 2215050 | A | 19960223 | 200104 | |
| | | | WO 96US2477 | A | 19960223 | | |

Priority Applications (No Type Date): US 95402176 A 19950310
Cited Patents: 2.Jnl.Ref; US 5315658; US 5519778
Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| WO 9628913 | A1 | E | 29 | H04K-001/00 | |
| Designated States (National): CA JP | | | | | |
| Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE | | | | | |
| US 5633928 | A | | 12 | H04L-009/00 | |
| EP 872064 | A1 | E | | H04K-001/00 | Based on patent WO 9628913 |
| Designated States (Regional): BE DE FR GB IT NL SE | | | | | |
| JP 11502035 | W | | 29 | G09C-001/00 | Based on patent WO 9628913 |
| CA 2215050 | C | E | | H04L-009/14 | Based on patent WO 9628913 |

Abstract (Basic): WO 9628913 A

The method for ensuring limited privacy in a communications network comprises sending from a terminal of a user or party 'a' via a network a cipher text message of the form c(a,b,d) = F(S(a,b,d),k(a,b,d)) to a number of parties 'b'.

P(a) is a **public key** of the party 'a', and S(a) is a secret key of party 'a'. A function g[S(a)] = P(a) mod p, where p and g are integers. P(b) is a **public key** of party 'b', and h is a one-way hash function. The term f indicates a has function abd d is a time interval. The term S(a,d) = H(S(a),d), and

S(a,b,d) = h(S(a,d), P(b)), and k(a,b,d) = h(P(b)[S(a)], d) and is a **session key** valid for a time d.

USE/ADVANTAGE - Facilitates warrants for wire-tapping for bounded time periods. Provides reasonable protection against misuse, greater privacy protection and more effective law enforcement. Can be used to target certain parties.

Dwg.1/3

Abstract (Equivalent): US 5633928 A

A method for assuring limited privacy in a communications network, comprising the steps of:

(a) sending a cipher message c=f(k,m) generated from a clear text message m via said network from a party a to a party b, said cipher message c including a **common session key** k of the parties a and b which is encrypted using a cipher function f and a cipher key which is derived from a secret key of the party a by the party a using a one way hash function;

(b) at least one trustee providing to a wiretapper terminal connected to said network sufficient information to permit said wiretapper terminal to decrypt said cipher message using said cipher key and obtain said **session key** without said wiretapper terminal obtaining said secret key of the party a;

(c) transmitting an information message via said network between

said parties a and b, the message being encrypted using said cipher function f and said **session key** ; and

(d) decrypting said information message transmitted between said parties a and b at said wiretapper terminal.

Dwg.2/3

Title Terms: KEY; ENCRYPTION; METHOD; TELECOMMUNICATION; METHOD; ENABLE; WIRE; TAP; DEFINE; SESSION; KEY; PUBLIC; SECRET; KEY; MONITOR; MONITOR; PARTY; RESPECTIVE; VALID; SET; TIME; INTERVAL

Derwent Class: P85; W01

International Patent Class (Main): G09C-001/00; H04K-001/00; H04L-009/00; H04L-009/14

International Patent Class (Additional): H04L-009/08; H04L-009/30; H04Q-007/38

File Segment: EPI; EngPI

Manual Codes (EPI/S-X): W01-A05A

**12/9/9 (Item 9 from file: 350)**

DIALOG(R)File 350:Derwent WPIX



010742143 **Image available**

WPI Acc No: 1996-239098/199624

XRPX Acc No: N96-200169

**Secure communication over insecure channels using public keyed methods - computing cryptovariable from information associated with certificates exchanged between node and terminal, second variable from prior art exchange and third from both of these**

Patent Assignee: AT & T CORP (AMTT )

Inventor: FAUCHER D W

Number of Countries: 001 Number of Patents: 001

Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week | |
|---|---|---|---|---|---|---|---|
| US 5515441 | A | 19960507 | US 94241534 | A | 19940512 | 199624 | B |

Priority Applications (No Type Date): US 94241534 A 19940512

Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| US 5515441 | A | | 19 | H04L-009/30 | |

Abstract (Basic): US 5515441 A

The method for securing communications involves storing a set of universal vectors obtained from a Key Certification Authority (KCA) at both the node and a communicating terminal. A node certificate obtained from the KCA including a KCA-certified digital signature, a node **public key** and a terminal identification (ID) are transmitted from the node to the communicating terminal. It is verified in the communicating terminal, from the set of universal vectors stored there, that the node certificate was obtained from the KCA. A terminal secret key is retrieved in the communicating terminal and used to generate a terminal **public key** . The terminal **public key** is transmitted from the communicating terminal to the node.

A first session cryptovariable is computed in the terminal from the node **public key** and the terminal secret key. The first session cryptovariable is computed in the node from the terminal **public key** and a node secret key associated with the node certificate. A **public key** exchange is performed between the node and the communicating terminal and a second session cryptovariable is computed from them in the node and in the communicating terminal. A **common session key** is computed from two cryptovariables. Messages exchanged between the

node and the communicating terminal are encrypted and decrypted using the **common session key** .
ADVANTAGE - Guards against man-in-middle attack.
Dwg.4/9
Title Terms: SECURE; COMMUNICATE; CHANNEL; PUBLIC; KEY; METHOD; COMPUTATION ; INFORMATION; ASSOCIATE; CERTIFY; EXCHANGE; NODE; TERMINAL; SECOND; VARIABLE; PRIOR; ART; EXCHANGE; THIRD
Derwent Class: W01
International Patent Class (Main): H04L-009/30
File Segment: EPI
Manual Codes (EPI/S-X): W01-A05B

**12/9/10 (Item 10 from file: 350)**
DIALOG(R)File 350:Derwent WPIX


009932869 **Image available**
WPI Acc No: 1994-200580/199424
XRPX Acc No: N94-157737
**Multiple source encryption of TV data - using separate encryption key for each source of data and** common **system** key **combined with individual keys**
Patent Assignee: SCIENTIFIC-ATLANTA INC (SCAT ); SCIENTIFIC ATLANTA INC (SCAT )
Inventor: GAMMIE K; WASILEWSKI A J
Number of Countries: 021 Number of Patents: 007
Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week |
|---|---|---|---|---|---|---|
| WO 9413081 | A1 | 19940609 | WO 93US11654 | A | 19931201 | 199424 B |
| US 5341425 | A | 19940823 | US 92984461 | A | 19921202 | 199433 |
| AU 9457345 | A | 19940622 | AU 9457345 | A | 19931201 | 199436 |
| EP 704123 | A1 | 19960403 | WO 93US11654 | A | 19931201 | 199618 |
| | | | EP 94903381 | A | 19931201 | |
| JP 8504308 | W | 19960507 | WO 93US11654 | A | 19931201 | 199646 |
| | | | JP 94513480 | A | 19931201 | |
| AU 685416 | B | 19980122 | AU 9457345 | A | 19931201 | 199811 |
| KR 299634 | B | 20011022 | WO 93US11654 | A | 19931201 | 200236 |
| | | | KR 95702231 | A | 19950602 | |

Priority Applications (No Type Date): US 92984461 A 19921202
Cited Patents: US 4531020; US 4605820; US 4613901; US 4634808; US 4803725; US 4887296; US 5029207; US 5093860; US 5115467; US 5144665; US 5144667; US 5237610
Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| WO 9413081 | A1 | E | 56 | H04L-009/18 | |
| Designated States (National): AU CA JP KR | | | | | |
| Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE | | | | | |
| US 5341425 | A | | 17 | H04L-009/18 | |
| AU 9457345 | A | | | H04L-009/18 | Based on patent WO 9413081 |
| EP 704123 | A1 | E | 1 | H04L-009/18 | Based on patent WO 9413081 |
| Designated States (Regional): DE FR GB IT | | | | | |
| JP 8504308 | W | | 54 | H04L-009/28 | Based on patent WO 9413081 |
| AU 685416 | B | | | H04L-009/18 | Previous Publ. patent AU 9457345<br>Based on patent WO 9413081 |
| KR 299634 | B | | | H04L-009/18 | Previous Publ. patent KR 95704881<br>Based on patent WO 9413081 |

Abstract (Basic): WO 9413081 A
The method involves providing each transmitting source with an

encryption key of B bits. Additionally a common system encryption key is provided using S bits. The **two keys** are combined in a defined way to form the actual encryption key used of E bits.

Each channel source (22..28) applies the combined key to its data before transmission (56). A receiver (30) is provided with both the system key and keys for one or more of the transmission sources. These keys are held in secure memory but require only ((N . B) + S) bits of data for N transmission sources.

USE/ADVANTAGE - For protecting digital information and unauthorised access e.g. subscription TV. Reduces amount of secure memory required in receivers to hold security keys.

Dwg.2/5

Abstract (Equivalent): US 5341425 A

A system key has a number (S) of bits and each of several broadcast keys comprises a unique group (B) of bits, where B is less than S. Convolving in a predetermined manner is carried out at each transmission site to generate a unique **data** encryption **key** for that transmission site. The set of data at each transmission site is encrypted with the unique **data** encryption **key** generated at that site.

The sets of data uniquely encrypted at each transmission site are then transmitted to the reception site. There is stored, in a memory at the reception site, the system key and one of the broadcast keys to enable a selected one of the encrypted sets of data to be decrypted at the reception site. The memory capacity necessary to store the system key and the broadcast keys at the reception site is no greater than ((Nmultiplied byB)+S) bits.

Dwg.2/5

Title Terms: MULTIPLE; SOURCE; ENCRYPTION; TELEVISION; DATA; SEPARATE; ENCRYPTION; KEY; SOURCE; DATA; COMMON; SYSTEM; KEY; COMBINATION; INDIVIDUAL; KEY

Derwent Class: P85; W01

International Patent Class (Main): H04L-009/18; H04L-009/28

International Patent Class (Additional): G09C-001/00; H04H-001/00; H04N-007/167

File Segment: EPI; EngPI

Manual Codes (EPI/S-X): W01-A05A

**12/9/11 (Item 11 from file: 350)**

DIALOG(R)File 350:Derwent WPIX



009573732 **Image available**

WPI Acc No: 1993-267278/199334

XRPX Acc No: N93-314371

Public key **encryption with elliptic curve for secure data communication - calculating between element and one of numerical data and identification code for prime number P defined over group of elements on curve**

Patent Assignee: MATSUSHITA ELEC IND CO LTD (MATU )

Inventor: MIYAJI A; TATEBAYASHI M

Number of Countries: 002 Number of Patents: 003

Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week | |
|---|---|---|---|---|---|---|---|
| JP 5181418 | A | 19930723 | JP 92168007 | A | 19920625 | 199334 | B |
| US 5272755 | A | 19931221 | US 92904944 | A | 19920626 | 199351 | |
| US 5351297 | A | 19940927 | US 92904944 | A | 19920626 | 199438 | |
| | | | US 9348478 | A | 19930416 | | |

Priority Applications (No Type Date): JP 91158205 A 19910628

Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| JP 5181418 | A | | 18 | G09C-001/00 | |
| US 5272755 | A | | 18 | H04L-027/30 | |
| US 5351297 | A | | 15 | H04K-001/00 | CIP of application US 92904944<br>CIP of patent US 5272755 |


Abstract (Basic): JP 5181418 A

Dwg.8/8

US 5272755 A

The method involves informing public data, and selecting two privacy keys at the end of two users. Numbers calculated by the public data and the privacy keys are mutually notified, and a **common key** is calculated by using the first privacy key and the number from the second user or by using the second privacy key and the number from the first user. Transmission **data** is **ciphered** using the **common key** by either user, and the ciphered data is deciphered using the **common key** by the other use.

Informing public data includes choosing d as a positive integer such that gives an imaginary quadratic field Q((-d))1/2) a small class number, choosing p as a prime number such that 4*p-1=d*square number, so that an elliptic curve E over GF(p) will have a j-invariant as a solution module p for a class polynomial Hd(x)=0 which is fixed by d. An order of a point other than a zero element is found from E1(GF(p)), and an elliptic curve E is chosen over (GF(p)) having an exact p order. An element other than the zero element of E(GF(p)) is chosen as a base point.

USE/ADVANTAGE - E.g. on public or broadcast network. E.g. rental laser disks. Uses elliptic curve to which MOV redn. cannot be applied. Field of definition can provide as many curves as number of bits. (First major country equivalent to JP5181418 A)

Dwg.8/8

Abstract (Equivalent): US 5351297 A

The method comprises the steps of supplying on the network system, public data to each of the users from the provider and selecting a first privacy key at a terminal of a first user and selecting a second privacy key at a terminal of a second user wherein the first and second privacy keys are different. It involves notifying a number calculated with the public data and the first privacy key to the second user from the first user and notifying a number calculated with the public data and the second privacy key to the first user from the second user. It involves generating a random number at the site of one of the first and second users who wishes to transmit a message and subsequently ciphering the random number with the public data.

The method then involves ciphering the message to be transmitted at the site of one of the first and second users who wishes to transmit the message by using the random number and the number notified from the other user. The ciphered random number and the ciphered message is then transmitted from the site of one of the first and second users who wishes to transmit the message to the other user. It involves deciphering the ciphered message using the privacy key and the ciphered random number at the site of the other user.

USE - For applying a **public key** encryption network system to users from a provider by using an elliptic curve, i.e. to provide security for information transmission.

Dwg.3/7


Title Terms: PUBLIC; KEY; ENCRYPTION; ELLIPSE; CURVE; SECURE; DATA; COMMUNICATE; CALCULATE; ELEMENT; ONE; NUMERIC; DATA; IDENTIFY; CODE; PRIME; NUMBER; P; DEFINE; GROUP; ELEMENT; CURVE

Index Terms/Additional Words: CABLE; RADIO; FACSIMILE

Derwent Class: P85; T01; W01; W02

International Patent Class (Main): G09C-001/00; H04K-001/00; H04L-027/30
International Patent Class (Additional): H04L-009/06; H04L-009/14
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): T01-J04A; T01-J12C; W01-A05A; T01-D01; T01-H07C; W01-A09D; W02-D; W02-F05A1A

**12/9/12 (Item 12 from file: 350)**
DIALOG(R)File 350:Derwent WPIX


009180697 **Image available**
WPI Acc No: 1992-308132/199237
XRPX Acc No: N92-235907

**Data processing system with communication nodes - has encryption device which encode data block which is then transmitted to other node to be received and decoded by decryption circuit**

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC ); IBM CORP (IBMC )
Inventor: JOHNSON D B; LE A V; MATYAS S M; PRYMAK R; WILKINS J D; MARTIN W C; ROHLAND W S
Number of Countries: 011 Number of Patents: 008
Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week | |
|---|---|---|---|---|---|---|---|
| US 5142578 | A | 19920825 | US 91748407 | A | 19910822 | 199237 | B |
| EP 529261 | A2 | 19930303 | EP 92111758 | A | 19920710 | 199309 | |
| CA 2068488 | A | 19930223 | CA 2068488 | A | 19920512 | 199319 | |
| EP 529261 | A3 | 19931118 | EP 92111758 | A | 19920710 | 199512 | |
| JP 7202878 | A | 19950804 | JP 92208406 | A | 19920713 | 199540 | |
| EP 529261 | B1 | 19970212 | EP 92111758 | A | 19920710 | 199712 | |
| DE 69217428 | E | 19970327 | DE 617428 | A | 19920710 | 199718 | |
| | | | EP 92111758 | A | 19920710 | | |
| CA 2068488 | C | 19980519 | CA 2068488 | A | 19920512 | 199831 | |

Priority Applications (No Type Date): US 91748407 A 19910822
Cited Patents: No-SR.Pub; 2.Jnl.Ref; EP 354770; EP 356065; JP 3128541; US 4924515; US 4941176
Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| US 5142578 | A | | 25 | H04L-009/30 | |
| EP 529261 | A2 | E | 35 | H04L-009/08 | |
| Designated States (Regional): CH DE FR GB IT LI NL SE | | | | | |
| JP 7202878 | A | | 21 | H04L-009/06 | |
| EP 529261 | B1 | E | 45 | H04L-009/08 | |
| Designated States (Regional): CH DE FR GB IT LI NL SE | | | | | |
| DE 69217428 | E | | | H04L-009/08 | Based on patent EP 529261 |
| CA 2068488 | A | | | G06F-013/38 | |
| EP 529261 | A3 | | | H04L-009/30 | |
| CA 2068488 | C | | | G06F-013/38 | |

Abstract (Basic): US 5142578 A

The apparatus distributes an initial **Data** Encryption **Algorithm** (DEA) key-encrypting key to encrypting a key record using a **public key algorithm** and a **public key** belonging to the intended recipient of the key record. The apparatus recovers the distributed key-encrypting key by the recipient by decrypting the received key record using the same **public key algorithm** and private key associated with the **public key** and re-encrypting the key-encrypting key under a key formed by arithmetically combining the recipient's **master key** with a control vector contained in the control information of the received key record.

The type and usage attributes assigned by the originator of the key-encrypting key in the form of a control vector are cryptographically coupled to the key-encrypting key such that the recipient may only use the received key-encrypting key in a manner defined by the key originator.

ADVANTAGE - Enhances security.

Dwg.15/16

Abstract (Equivalent): EP 529261 B

An apparatus for enabling a first node (20) of a pair of nodes to control a crypto variable after its transmission from said first node (20) to a second node (20') of said pair of nodes, in a data processing system (10) having a plurality of communicating nodes (20,20',20''), at least one pair of nodes (20,20') in the system (10) exchanging cryptographic communications, said apparatus is comprising: a first storage means (40) at a transmitting node (20) in the system (10) for storing a crypto variable which is to be transmitted to a receiving node (20') in the system (10); a second storage means at said transmitting node (20) for storing control information (60) to control said crypto variable after it is transmitted from said transmitting node (20), said control information (60) including a control vector to limit the uses of said crypto variable; a third storage means at said transmitting node (20) for storing a first key expression; concatenating means (42) at said transmitting node (20) coupled to said first (40) and second storage means, for concatenating said crypto variable with said control information (60), forming a key block (80); encryption means (44) at said transmitting node (20), coupled to said third storage means and said concatenating means (42), for encrypting said key block (80) with said first key expression, forming an encrypted key block (85); and transmitting means (46) at said transmitting node (20) coupled to said encryption means (44) and coupled over a communications link to a receiving means at said receiving node (20'), for transmitting said encrypted key block (85) to said receiving node (20'); and said apparatus is characterised by: said transmitting means (46) coupled to said second storage means, for transmitting an unencrypted copy of said control information to said receiving node (20'); fourth storage means at said receiving node (20'), for storing a second key expression corresponding to said first key expression; decryption means (54) at said receiving node (20') coupled to said receiving means and to said fourth storage means, for decrypting said encrypted key block (85) using said second key expression, to obtain a recovered key block; extraction means (52) at said receiving node (20') coupled to said decryption means (54), to extract said control information (60) and said crypto variable from said recovered key block; comparison means (59) at said receiving node (20') coupled to said extraction means (52) and coupled to said receiving means for comparing said control information (60) extracted from said recovered key block to said unencrypted copy of said control information (60), said comparison means (59) having an enabling output for signalling if said comparison shows equality; control means coupled to said extraction means (52) and having an enabling input coupled to said enabling output of said comparison means (59), for controlling storage of said crypto variable with said control information (60).

Dwg.1/16

Title Terms: DATA; PROCESS; SYSTEM; COMMUNICATE; NODE; ENCRYPTION; DEVICE; ENCODE; DATA; BLOCK; TRANSMIT; NODE; RECEIVE; DECODE; DECRYPTER; CIRCUIT

Derwent Class: P85; W01

International Patent Class (Main): G06F-013/38; H04L-009/06; H04L-009/08; H04L-009/30

International Patent Class (Additional): G09C-001/00; H04L-009/14

File Segment: EPI; EngPI

Manual Codes (EPI/S-X): W01-A05A

12/9/13 (Item 13 from file: 350)
DIALOG(R)File 350:Derwent WPIX


008712830 **Image available**
WPI Acc No: 1991-216849/199130
Related WPI Acc No: 2002-368982
XRPX Acc No: N91-165483

**Multi-media network system for TV video signal - puts digital signature for certifying transmission source simultaneously with encryption when files are transmitted**

Patent Assignee: CANON KK (CANO )
Inventor: NAKAMURA K
Number of Countries: 008 Number of Patents: 007
Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week | |
|---|---|---|---|---|---|---|---|
| EP 438154 | A | 19910724 | EP 91100521 | A | 19910117 | 199130 | B |
| JP 3214834 | A | 19910920 | JP 908366 | A | 19900119 | 199144 | |
| US 5159633 | A | 19921027 | US 91641879 | A | 19910115 | 199246 | |
| EP 438154 | A3 | 19920722 | EP 91100521 | A | 19910117 | 199335 | |
| EP 438154 | B1 | 19970716 | EP 91100521 | A | 19910117 | 199733 | |
| DE 69126801 | E | 19970821 | DE 626801 | A | 19910117 | 199739 | |
| | | | EP 91100521 | A | 19910117 | | |
| JP 2000206877 | A | 20000728 | JP 908366 | A | 19900119 | 200041 | |
| | | | JP 200035457 | A | 19900119 | | |

Priority Applications (No Type Date): JP 908366 A 19900119; JP 200035457 A 19900119
Cited Patents: NoSR.Pub; 1.Jnl.Ref; EP 179612; GB 2161680; WO 8500718; WO 8806826
Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| EP 438154 | A | | | | |
| Designated States (Regional): DE FR GB IT NL SE | | | | | |
| US 5159633 | A | | 18 | H04L-009/30 | |
| EP 438154 | B1 | E | 24 | H04N-007/167 | |
| Designated States (Regional): DE FR GB IT NL SE | | | | | |
| DE 69126801 | E | | | H04N-007/167 | Based on patent EP 438154 |
| JP 2000206877 | A | | 12 | G09C-001/00 | Div ex application JP 908366 |

Abstract (Basic): EP 438154 A

The network system comprises a transmitting terminal comprising a secret-key encryptor for encrypting the real-time communication type information by a secret-key system in which only transmitting and receiving terminals of the information have encryption and decryption keys. A **public - key** encryptor encrypts the storage type information by a **public - key** system in which all the terminals commonly have their own encryption keys.

Only a receiving terminal of the information has its own decryption key. A first secret-key control causes the secret-key encryptor to change a **common** encryption **key** in each communication, and causes the **public - key** encryptor to encrypt and transmit the changed key.

ADVANTAGE - High speed transmission. (19pp Dwg.No.2/8

Abstract (Equivalent): EP 438154 B

A multimedia network system for transmitting real-time data such as a television video signal and stored data such as a computer file using at least one transmission path, comprising: a transmitting terminal (1) comprising a secret-key encryption means (108, 109, 110; 72, 73, 75)

for encrypting the real-time data by a secret-key system in which data transmitting terminals and data receiving terminals both know the secret-key used for encryption and decryption of transmitted data; a **public - key** encryption means (103) for encrypting the stored data by a **public - key** system in which the encryption key of each terminal is commonly accessible but the decryption key of each terminal is held private by each corresponding terminal, and a first secret-key control means (101, **DATA KEY** ; 74) for causing said secret-key encryption means to change the secret-key, characterised in that said first secret-key control means causes said **public - key** encryption means to encrypt and transmit the changed secret-key and causes said secret-key encryption means to change the secret-key in response to the reception of a data transmission request from a receiving terminal each time such a data transmission request is received.

Dwg.1a/8

Abstract (Equivalent): US 5159633 A

The multimedia network system transmits real-time communication type information such as a television video signal and storage type information such as a computer file using at least one transmission path. The real-time communication type information is encrypted by a secret-key system, and the storage type information is encrypted by a **public - key** system.

A **common** encryption **key** of the **public - key** system is changed in each communication.

USE/ADVANTAGE - For optical-fibre networks. LANs etc. transmitting video or computer signals. Allows encryption of high-speed information.

Dwg.1A/8

Title Terms: MULTI; MEDIUM; NETWORK; SYSTEM; TELEVISION; VIDEO; SIGNAL; DIGITAL; SIGNATURE; CERTIFY; TRANSMISSION; SOURCE; SIMULTANEOUS; ENCRYPTION; FILE; TRANSMIT

Derwent Class: P85; W01; W02

International Patent Class (Main): G09C-001/00; H04L-009/30; H04N-007/167

International Patent Class (Additional): H04L-009/06; H04L-009/32; H04N-007/16

File Segment: EPI; EngPI

Manual Codes (EPI/S-X): W01-A05; W01-A06C; W02-F03A; W02-F05A; W02-L

**12/9/14 (Item 14 from file: 350)**

DIALOG(R)File 350:Derwent WPIX



008410724 **Image available**

WPI Acc No: 1990-297725/199039

XRPX Acc No: N90-228840

**Cryptographic for** public key **exchange with authentication - two user devices establish** common session key **by exchanging information over insecure communication channel**

Patent Assignee: TRW INC (THOP )

Inventor: GOSS K C

Number of Countries: 007 Number of Patents: 004

Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week | |
|---|---|---|---|---|---|---|---|
| US 4956863 | A | 19900911 | US 89339555 | A | 19890417 | 199039 | B |
| EP 393806 | A | 19901024 | EP 90300115 | A | 19900105 | 199043 | |
| JP 2288746 | A | 19901128 | JP 90233578 | A | 19900214 | 199103 | |
| CA 2024049 | A | 19920228 | CA 2024049 | A | 19900827 | 199220 | |

Priority Applications (No Type Date): US 89339555 A 19890417

Cited Patents: 1.Jnl.Ref; A3...9146; NoSR.Pub; US 4200770
Patent Details:
Patent No Kind Lan Pg Main IPC Filing Notes
EP 393806 A
Designated States (Regional): DE FR GB IT
CA 2024049 A H03M-007/00

Abstract (Basic): EP 393806 A

Each device has a previously stored unique random number Xi, and a previously stored composite quantity that is formed by transforming Xi to Yi using a transformation of which the inverse in computationally infeasible.

Yi is concatenated with a publicly known device identifier, and the quantity is digitally signed. Before a communication session is established, two user devices exchange their signed composite quantities, transform them to unsigned form, and authenticate the identity of the other user. Then each device generates the same **session key** by transforming the received Y value with its own X value. For further security, each device also generates another random number X'i, which is transformed to a corresp. number Y'i. These Y'i values are also exchanged, and the **session key** is generated in each device, using a transformation that involves the device's own Xi and Y'i number and the Yi and Y'i numbers received from the other device.

USE/ADVANTAGE - Cryptographic systems. Accomplishes both secrecy and identity authentication without need for key distribution centre.

(12pp Dwg.No.3/5

Abstract (Equivalent): US 4956863 A

Each device has a previously stored unique random number Xi, and a previously stored composite quantity that is formed by transforming Xi to Yi using a transformation of which the inverse in computationally infeasible. Yi is concatenated with a publicly known device identifier, and the quantity is digitally signed. Before a communication session is established, two user devices exchange their signed composite quantities, transform them to unsigned form, and authenticate the identity of the other user.

Then each device generates the same **session key** by transforming the received Y value with its own X value. For further security, each device also generates another random number X'i, which is transformed to a corresp. number Y'i. These Y'i values are also exchanged, and the **session key** is generated in each device, using a transformation that involves the device's own Xi and Y'i number and the Yi and Y'i numbers received from the other device.

USE/ADVANTAGE - Cryptographic systems. Accomplishes both secrecy and identity authentication without need for key distribution centre.

(12pp Dwg.No.3/5

Title Terms: CRYPTOGRAPHIC; PUBLIC; KEY; EXCHANGE; AUTHENTICITY; TWO; USER; DEVICE; ESTABLISH; COMMON; SESSION; KEY; EXCHANGE; INFORMATION; COMMUNICATE; CHANNEL
Derwent Class: P85; W01
International Patent Class (Main): H03M-007/00
International Patent Class (Additional): G09C-001/00; H04K-001/00; H04L-009/32
File Segment: EPI; EngPI
Manual Codes (EPI/S-X): W01-A05

**12/9/15 (Item 15 from file: 350)**
DIALOG(R)File 350:Derwent WPIX


004156519

WPI Acc No: 1984-302058/198449
XRPX Acc No: N84-225228

**Television scrambling with remote selective de-scrambling - is for subscription TV system using several levels of encryption algorithm**

Patent Assignee: CABLE HOME COMMUNICATION CORP (CABL-N); TITAN CORP (TITA-N); CABLE/HOME COMMUNICATION (CABL-N); MA-COM LINKABIT (MACO-N)
Inventor: GILHOUSEN K S; MOERDER K E; NEWBY C F; GILHOUSER K S
Number of Countries: 013 Number of Patents: 012
Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week |
|---|---|---|---|---|---|---|
| EP 127381 | A | 19841205 | EP 84303320 | A | 19840516 | 198449 B |
| AU 8428707 | A | 19841129 | | | | 198504 |
| NO 8402067 | A | 19841227 | | | | 198507 |
| DK 8402554 | A | 19841128 | | | | 198513 |
| JP 60057783 | A | 19850403 | JP 84106346 | A | 19840525 | 198520 |
| US 4613901 | A | 19860923 | US 83498800 | A | 19830527 | 198641 |
| EP 127381 | B | 19880406 | | | | 198814 |
| DE 3470368 | G | 19880511 | | | | 198820 |
| CA 1242793 | A | 19881004 | | | | 198844 |
| CA 1264848. | A | 19900123 | | | | 199008 |
| JP 2096489 | A | 19900409 | JP 84330725 | A | 19840525 | 199020 |
| DK 167332 | B | 19931011 | DK 842554 | A | 19840524 | 199346 |

Priority Applications (No Type Date): US 83498800 A 19830527
Cited Patents: GB 1590579; US 3789131; US 4245246; US 4292650
Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| EP 127381 | A | E | 82 | | |
| Designated States (Regional): BE DE FR GB IT NL SE | | | | | |
| EP 127381 | B | E | | | |
| Designated States (Regional): BE DE FR GB IT NL SE | | | | | |
| DK 167332 | B | | | H04N-007/167 | patent DK 8402554 |

Abstract (Basic): EP 127381 A

A working key signal is generated by processing an initialisation vector signal in accordance with the DES algorithm on the algorithm being keyed by a **common** category **key** signal or a signal having a predetermined relationship to this signal. A unique encryptation key stream is generated on processing the initialisation vector signal in accordance with DES algorithm on the algorithm being keyed by the working key signal. The TV signal is scrambled in accordance with the key stream.

A number of unique encrypted category key signals individually addressed to selected subscribers descrambles are operated by processing the initial **common** category **key** signal in accordance with the DES algorithm. The algorithm is keyed by a number of different unit key signals unique to different selected descramblers. The scrambled signal, initialisation vector signal and encrypted category key signals are broadcast to the descramblers. The descrambler uses a corresponding tier of DES algorithms to reproduce the encryptation key stream which is used to descramble the TV signal. Each descrambler has its unique unit key signal stored in a secure memory. This is for use in **reproducing** the **common category key** signal when the descrambler is addressed by its unique encrypted category key signal.

ADVANTAGE - The system is highly secure against unauthorised descrambling. At least three levels of encryptation algorithms are used in the scrambling and descrambling

Abstract (Equivalent): EP 127381 B

A working key signal is generated by processing an initialisation vector signal in accordance with the DES algorithm on the algorithm being keyed by a **common** category **key** signal or a signal having a

predetermined relationship to this signal. A unique encryptation key stream is generated on processing the initialisation vector signal in accordance with DES algorithm on the algorithm being keyed by the working key signal. The TV signal is scrambled in accordance with the key stream.

A number of unique encrypted category key signals individually addressed to selected subscribers descrambles are operated by processing the initial **common** category **key** signal in accordance with the DES algorithm. The algorithm is keyed by a number of different unit key signals unique to different selected descramblers. The scrambled signal, initialisation vector signal and encrypted category key signals are broadcast to the descramblers. The descrambler uses a corresponding tier of DES algorithms to reproduce the encryptation key stream which is used to descramble the TV signal. Each descrambler has its unique unit key signal stored in a secure memory. This is for use in **reproducing** the **common category key** signal when the descrambler is addressed by its unique encrypted category key signal.

ADVANTAGE - The system is highly secure against unauthorised descrambling. At least three levels of encryptation algorithms are used in the scrambling and descrambling.

Dwg.0/8

Abstract (Equivalent): US 4613901 A

A working key signal is generated by processing an ''initialisation vector'' signal in accordance with the DES algorithm upon the algorithm being keyed by either a **common** category **key** signal or some other key signal. A unique encryption keystream is generated by processing the initialisation vector signal in accordance with the DES algorithm upon the algorithm being keyed by the working key signal. A television signal is scrambled in accordance with the unique encryption keystream to provide a scrambled television signal. A number of unique encrypted category key signals individually addressed to different selected subscribers' descramblers are generated by processing the initial **common** category **key** signal in accordance with the DES algorithm upon the algorithm being keyed by a plurality of different ''unit key'' signals unique to different selected descramblers. The scrambled television signal, the initialisation vector signal, and the encrypted category key signals are broadcast to the descramblers.

A corresponding tier of DES algorithms are employed at the descrambler to reproduce the encryption keystream; and the TV signal is descrambled. Each descrambler has its unique unit key signal stored in a secure memory for use in **reproducing** the **common category key** signal when the descrambler is addressed by its unique encrypted category key signal.

(26pp

Title Terms: TELEVISION; SCRAMBLE; REMOTE; SELECT; DE; SCRAMBLE; SUBSCRIBER ; TELEVISION; SYSTEM; LEVEL; ENCRYPTION; ALGORITHM

Derwent Class: W02

International Patent Class (Main): H04N-007/167

International Patent Class (Additional): H04K-001/00; H04L-009/00; H04N-007/16

File Segment: EPI

Manual Codes (EPI/S-X): W02-F05; W02-L

**12/9/16 (Item 16 from file: 347)**

DIALOG(R)File 347:JAPIO



07360952 **Image available**

METHOD AND SYSTEM FOR AUTHENTICATING DATA

PUB. NO.: 2002-229449 [JP 2002229449 A]
PUBLISHED: August 14, 2002 (20020814)
INVENTOR(s): MAEDA KENICHI
APPLICANT(s): NETTIME CORP
APPL. NO.: 2001-022800 [JP 20011022800]
FILED: January 31, 2001 (20010131)
INTL CLASS: G09C-001/00; G06F-012/14; H04L-009/08

ABSTRACT

PROBLEM TO BE SOLVED: To enhance the reliability of communication data transmitted to a server 2 from a user terminal 5 through networks 4, 3, 6, and 1.

SOLUTION: The communication data received by the server 2 are transferred to another server 6, and receipt time in the other server 6 is made to reply with the communication data (time authentication). The user terminal 5 encrypts the communication data by using a **session key** created from a **common key** and random numbers. The random numbers and the encrypted result are transmitted to the server 2 with the communication data, and the server 2 also performs the same processing by using the **common key** (tampering prevention). In the user terminal 5, the communication data are encrypted with the created **session key** , the **session key** is encrypted with a secret key and transmitted. The server 2 decrypts the **session key** and the communication data with a **public key** , and decides the coincidence between the signature encrypted with the communication data and the received signature (tampering prevention, improvement of data secrecy).



**12/9/17 (Item 17 from file: 347)**
DIALOG(R)File 347:JAPIO


07353660 **Image available**
METHOD AND DEVICE FOR TRANSMITTING ELECTRONIC MAIL

PUB. NO.: 2002-222151 [JP 2002222151 A]
PUBLISHED: August 09, 2002 (20020809)
INVENTOR(s): TANIMOTO YOSHIFUMI
APPLICANT(s): MURATA MACH LTD
APPL. NO.: 2001-017517 [JP 20011017517]
FILED: January 25, 2001 (20010125)
INTL CLASS: G06F-013/00

ABSTRACT

PROBLEM TO BE SOLVED: To efficiently broadcast an electronic mail containing an enciphered data.

SOLUTION: A personal computer PC1 generates a **session key** when receiving from a user an indication that the same data is transmitted to plural addresses by the electronic mail (S105), and enciphers the data using the generated **session key** (S106). A **common key** is generated using a **public key** generated based on each electronic mail address of the addresses and a private key acquired preliminarily from a center (S107), and enciphers the **session key** using the generated **common key** (S108). The electronic mail containing the enciphered data and the **session key** is transmitted to the respective addresses (S110).

**12/9/18 (Item 18 from file: 347)**
DIALOG(R)File 347:JAPIO


07349399 **Image available**
METHOD OF FINDING REPLICATED TERMINAL

PUB. NO.: 2002-217890 [JP 2002217890 A]
PUBLISHED: August 02, 2002 (20020802)
INVENTOR(s): MATSUZAKI NATSUME
ANZAI JUN
MATSUMOTO TSUTOMU
APPLICANT(s): ADVANCED MOBILE TELECOMMUNICATIONS SECURITY TECHNOLOGY RESEARCH LAB CO LTD
APPL. NO.: 2001-013250 [JP 20011013250]
FILED: January 22, 2001 (20010122)
INTL CLASS: H04L-009/08; G09C-001/00; H04L-009/32

ABSTRACT

PROBLEM TO BE SOLVED: To automatically find and exclude a replicated terminal in a communication system consisting of a center and a plurality of terminals.

SOLUTION: The center and a plurality of the terminal are connected through a communication network for ciphering communication with individual group keys. The center sends challenge information, in the case of delivering a new **group key** to the terminals. Each of the terminals sends response information obtained by ciphering terminal ID and a terminal random number to a center **public key** to the center, which retrieves a communication log to inspect the presence/absence of terminals, having the same terminal ID and different terminal random numbers. If there are corresponding terminals, it is determined that the replicated terminal exists, and the **session key** is not delivered. Since random number generated by an original terminal is difficult to replicate, the replicated terminal cannot generate the same random number, so that the existence of the replicated terminal can be detected. When the replicated terminal is found, the multi-address communication of exclusion information that this has been excluded is performed, to deliver the same group keys to unchecked terminals.



**12/9/19 (Item 19 from file: 347)**
DIALOG(R)File 347:JAPIO


06833450 **Image available**
CIPHER COMMUNICATION SYSTEM

PUB. NO.: 2001-060944 [JP 2001060944 A]
PUBLISHED: March 06, 2001 (20010306)
INVENTOR(s): IENAGA ITARU
APPLICANT(s): HITACHI LTD
APPL. NO.: 11-236763 [JP 99236763]
FILED: August 24, 1999 (19990824)
INTL CLASS: H04L-009/08; G06F-013/00; G09C-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To improve safety by eliminating previous setting of a **public key** , management of **public key** /secret key and a key registration center.

SOLUTION: A prime generation part 102 generates a random number R in a random number generation part 105 based on session information (t) with respect to transmission side identification information IDa and reception side identification information IDb and generates a large prime. A **session key** generation part 103 generates a cryptographic key K1 as a **session key** Ke based on the prime and file information F. A **master key** generation part 106 ciphers the plain sentence M110 of a file by the cryptographic key K1, generates a cipher sentence C112, decentralizes the cryptographic key K1 and generates two cryptographic keys a109 and b108. A mail control part 104 adds a cryptographic key a 112 to the cipher sentence C112, transmits it to a user B as a mail main body, adds the cryptographic key b108 to the mail to which a **session key** Ke 107, session information (t) and file information F are added and sends the mail later as an auxiliary mail.



**12/9/20 (Item 20 from file: 347)**



06598069 **Image available**

METHOD AND SYSTEM FOR CIPHER COMMUNICATION, AND RECORDING MEDIUM STORED WITH CIPHER COMMUNICATION PROGRAM

PUB. NO.: 2000-183866 [JP 2000183866 A]
PUBLISHED: June 30, 2000 (20000630)
INVENTOR(s): HATAJIMA TAKASHI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP (NTT)
APPL. NO.: 10-351857 [JP 98351857]
FILED: December 10, 1998 (19981210)
INTL CLASS: H04L-009/08; G09C-001/00; H04L-009/14

ABSTRACT

PROBLEM TO BE SOLVED: To confirm if a communication sentence is transferred to the other party being safe and legal by generating either a **common key** or a session ID and transmitting the communication text with either of them utilized for an electronic envelope.

SOLUTION: A transmission application part 11 of an entity A10 transmits destination information to a key server C20 and requests client authentication. A decoding part 13 of a **one** -time **common key** decodes a **one** -time **common key** Kc transmitted from the server C20 and takes out the key Kc. And, an electronic envelope preparing part 15 enters a communication text M of plaintext to be transmitted to a receiving client B by a transmitting client A into an electronic envelope E and directly transmits it to an entity B30 without going through the server C20. Further, a key use state managing part 25 issues a session ID which is generated by a random number generator including a session ID proper to this transaction and is enciphered to a **public key** with the **public key** Kpc of the server C20 and a **public key** Kpb of the transmission destination entity B30 in each transmission destination.

**12/9/21 (Item 21 from file: 347)**
DIALOG(R)File 347:JAPIO


06437113 **Image available**
DIGITAL CONTENTS DISTRIBUTION METHOD AND RECORDING MEDIUM REPRODUCIBLY RECORDING CONTENTS

PUB. NO.: 2000-022680 [JP 2000022680 A]
PUBLISHED: January 21, 2000 (20000121)
INVENTOR(s): ASADA KAZUNORI
APPLICANT(s): OPEN LOOP KK
APPL. NO.: 10-191706 [JP 98191706]
FILED: July 07, 1998 (19980707)
INTL CLASS: H04L-009/08; G06F-015/00; G06F-017/60; G09C-001/00

ABSTRACT

PROBLEM TO BE SOLVED: To prevent the unauthorized copy utilization of digital contents of music or the like and to safely distribute them.

SOLUTION: A management center 11 supplies a **master public key** KPUk to a contents maker and supplies a **master** private **key** KPRk to an LSI maker 15. The contents maker 13 records **data ciphered** by generating a contents cipher key Kco for the respective contents, the data for which the contents cipher key Kco is ciphered by the **master public key** KPUk, its own signature and a certificate DV from the management center 11 in this recording medium. The LSI maker 15 includes the **master** private **key** KPRk for decoding the ciphered contents cipher key in a decoding LSI. A decoding equipment decodes the contents cipher key by the **master** private **key** KPRk and decodes the contents at the time of judging that the certificate DV and signature DS of the mounted recording medium are both valid by the decoding LSI.



**12/9/22 (Item 22 from file: 347)**
DIALOG(R)File 347:JAPIO


06273528 **Image available**
KEY MANAGEMENT METHOD AND ITS SYSTEM

PUB. NO.: 11-215116 [JP 11215116 A]
PUBLISHED: August 06, 1999 (19990806)
INVENTOR(s): KURODA IKUKO
KANDA MASASUKI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT>
APPL. NO.: 10-013900 [JP 9813900]
FILED: January 27, 1998 (19980127)
INTL CLASS: H04L-009/08

ABSTRACT

PROBLEM TO BE SOLVED: To provide a key recovering method by which abuse of the rights by a law enforcing organ, a key management organ, and an international third organ can be prevented and a user is not allowed to invalidate the enforcement of a law.

SOLUTION: When a user A transmits information to another user B, the user A generates an international **master key** IKAB from the international open key of the user B and from the international secret key of the user A, enforcement agreement information ED by enciphering the **master key** IKAB and date hour information D, a session key KS from the information ED and from a national **common key** , and additional information INF by enciphering the **master key** IKAB with the open key PI of an organ 14, and adding the information INF to annexing information LEAF, and sends the information LEAF and a plaintext enciphered with the session key KS to the user B. The user B prepares the **master key** IKAB with the international open key of the user A and with the international secret key of the user B, additional information INF' by enciphering the **master key** IKAB with the open key PI of the organ 14, and, only when the information INF' coincides with the received information INF, prepares the session key KS. At the time of enforcing a law, an organ 15 sends the information LEAF to the organ 14 and the organ 14 obtains the **master key** IKAB by decoding the information INF with the international secret key of the organ 14, prepares the execution agreement information ED by using the key IKAB, and returns the information ED to the organ 15. The organ 15 sends the information LEAF and ED to an organ 12A and both organs 15 and 12 **copy** the **session key** KS by exchanging information between them.



**12/9/23 (Item 23 from file: 347)**


06085738 **Image available**
KEY RECOVERY SYSTEM, KEY RECOVERY DEVICE, RECORDING MEDIUM FOR STORING KEY RECOVERY PROGRAM AND KEY RECOVERY METHOD

PUB. NO.: 11-027253 [JP 11027253 A]
PUBLISHED: January 29, 1999 (19990129)
INVENTOR(s): DOMYO SEIICHI
TSUCHIYA HIROYOSHI
SUGANO KIYOKO
ANDO HIROYUKI
MORITA ICHIRO
KURODA YASUTSUGU
TORII NAOYA
MIYAUCHI HIROSHI
SAKO KAZUE
YAMAZAKI MASASHI
APPLICANT(s): HITACHI LTD
FUJITSU LTD
NEC CORP
APPL. NO.: 09-181189 [JP 97181189]
FILED: July 07, 1997 (19970707)
INTL CLASS: H04L-009/08

ABSTRACT

PROBLEM TO BE SOLVED: To attain efficient performance of a total key recovery system.

SOLUTION: This system is equipped with verifying devices 12a and 12b, which discriminate, in accordance with an identifier RCL1 attached to a cipher **data** (the **cipher** data obtained by ciphering the **common key** KS with a **public key** KRCpub) provided by a user's terminals 10a to 10d, whether

or not a user concerned has a recovery authority for a **common key** KS; and a key recovery device 14, which recovers the **common key** by decoding the cipher data with a private key KRCpri, a counterpart of the **public key** KRCpub, provided separately from verifying devices 12a and 12b. The verifying devices 12 and 12b provide the user concerned with the **common key** KS recovered by the key recovery device 14, only when it is discriminated that the user has the recovery authority.



**12/9/24 (Item 24 from file: 347)**
DIALOG(R)File 347:JAPIO


05679320 **Image available**
ACCESS CONTROL METHOD AND SYSTEM FOR CIPHERED SHARED DATA

PUB. NO.: 09-294120 [JP 9294120 A]
PUBLISHED: November 11, 1997 (19971111)
INVENTOR(s): SATO MAKOTO
NANBA AKIRA
DOMYO SEIICHI
TAKARAGI KAZUO
SHIBAHARA SETSUO
APPLICANT(s): HITACHI LTD [000510] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 08-107501 [JP 96107501]
FILED: April 26, 1996 (19960426)
INTL CLASS: [6] H04L-009/08; G09C-001/00; H04L-009/14
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.2 (COMMUNICATION -- Transmission Systems); 44.9 (COMMUNICATION -- Other); 45.4 (INFORMATION PROCESSING -- Computer Applications)

ABSTRACT

PROBLEM TO BE SOLVED: To allow user groups to share data with security by using a ciphering communication technology.

SOLUTION: A **data ciphering** section 14 and a **data key ciphering** section 15 of a terminal equipment 3 cipher data respectively by using a **data key** generated by a **data key** generating section 13 and use a **public key** 221 corresponding to a designated secrecy **group** to **cipher** the **data key** and a server 5 stores the data 211 and a **data key** 212. In the case of referencing the data 211, the terminal equipment 3 sends the acquired **data key** 212 and an open individual key 111 to the server 5, the server 5 uses a secret key to decode the **data key** 212 and uses the open individual key 111 to cipher the decoded **data key** and sends the result to the terminal equipment 3. A **data key** decoding section 17 uses a secret individual key 112 to decode the acquired **data key** and a data decoding section 18 decodes the data.

**12/9/25 (Item 25 from file: 347)**
DIALOG(R)File 347:JAPIO


02136142 **Image available**
DISTRIBUTING SYSTEM FOR CRYPTOGRAPHIC KEY

PUB. NO.: 62-053042 [JP 62053042 A]

PUBLISHED: March 07, 1987 (19870307)
INVENTOR(s): KOBAYASHI TETSUJI
OOTA KAZUO
APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 60-193483 [JP 85193483]
FILED: September 02, 1985 (19850902)
INTL CLASS: [4] H04L-009/02; G09C-001/00
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION -- Other)
JOURNAL: Section: E, Section No. 529, Vol. 11, No. 240, Pg. 118, August 06, 1987 (19870806)

ABSTRACT

PURPOSE: To prevent the effect of the processing speed of an RSA cryptology from being given onto the processing time of the session of the user by separating a key distributed in the RSA cryptology from a key distributed by a DES cryptology.

CONSTITUTION: A **data ciphering key** distribution key KN is ciphered by the RSA cryptology and distributed by using a **public key** PK. A **data ciphering key** KF is ciphered by a DES cryptology and distributed by using the key KN. The keys KN and KF are distributed independently timewise. The **master key** KM is used within each node to protect other code in each node. The secret key SK is used to decode the RSA cryptology.